UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,938	03/15/2004	G. Glenn Henry	CNTR.2072	1288

23669 7590 01/05/2010
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2432	
NOTIFICATION DATE	**DELIVERY MODE**
01/05/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/800,938	HENRY ET AL.	
	Examiner	**Art Unit**	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 25 October 2009 has been entered.

Response to Amendment

2. Applicant's amendment filed 25 October 2009 amends claims 1-3, 9, 12-14, 16, and 21. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant argues, "nowhere do these reference suggest that use of an x86-compatible microprocessor for purposes of performing an encryption operation…it does not follow that one skilled would be even remotely motivated to implement the x86 instruction set on the co-processor of Kessler for Kessler's co-processor only possesses those capabilities needed to perform security operations." This argument is not persuasive because Colavin discloses that the co-processor is more than just a simple co-processor that "only possesses those capabilities needed to perform security operations", but instead is reconfigurable to provide program executions with very high instruction level parallelism ([0084]).

4. Applicant argues, "The only contribution that Miller makes to the argument is that the x86 instruction set is well-known and widely accepted. Applicant concedes this point. However, that the x86 instruction set is well-known and widely accepted does not provide sufficient

motivation to add an estimated two orders of magnitude of functionality to a security co-processor interface in order to produce an x86-compatible microprocessor." This argument is not persuasive because the co-processor of Kessler as modified by Colavin would not be a mere "security co-processor" as alleged by Applicant (see response provided above). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14).

5. Applicant argues, "If the Examiner is suggesting that Colavin's co-processor executes portions of an application program, then Application agrees with this point, but like the citation of Miller, Applicant argues that such a combination does not have any practical relevance." This argument is not persuasive because it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor of Kessler to execute the actual application program as described by Colavin in order to efficiently execute programs with high instruction level parallelism as taught by Colavin ([0002]).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler, U.S. Patent No. 6,789,147, in view of Colavin, U.S. Publication No. 2004/0103263, and further in view of Miller, U.S. Patent No. 6,081,884. Referring to claims 1, 21, Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8 & Col. 4, lines 12-13), which meets the limitation of fetch logic, configured to receive a single, atomic cryptographic instruction as a part of an instruction flow executing on said microprocessor, wherein said single, atomic cryptographic instruction prescribes an encryption operation. The execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of wherein said single, atomic cryptographic instruction prescribes one of a plurality of cryptographic algorithms, algorithm logic, operatively coupled to said single, atomic cryptographic instruction, configured to direct said microprocessor to execute said encryption operation according to said one of a plurality of cryptographic algorithms. Using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9,

lines 28-43), which meets the limitation of execution logic, operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations. The operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4 (Figures 5 & 8), which meets the limitation of executing a plurality of cryptographic rounds required to complete said encryption operation. Kessler does not specify that the co-processor executes that program that includes the cryptographic operations. Colavin discloses a host and co-processor configuration wherein the co-processor executes the actual application program (Abstract & [0018]), which meets the limitation of said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application is executed by said microprocessor to obtain expected results. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor of Kessler to execute the actual application program as described by Colavin in order to efficiently execute programs with high instruction level parallelism as taught by Colavin ([0002]). Kessler does not specify that the co-processor utilizes the x86 instruction set. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14). Applicant's specification shows that integer instructions are inherent to the x86 instruction set (Page 27). Therefore, when implementing the x86 instruction set in the co-processor of Kessler, as previously described, the execution units would effectively operate as a "integer unit" as claimed.

Referring to claims 2, 3, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4 (Figures 5 & 8), which meets the limitation of said encryption operation comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks, a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

Referring to claims 4, 22, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as AES (Figures 5 & 8), which meets the limitation of one of a plurality of cryptographic algorithms comprises the Advanced Encryption Standard (AES) algorithm.

Referring to claims 5, 23, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as DES (Figures 5 & 8), which meets the limitation of one of a plurality of cryptographic algorithms comprises the Digital Encryption Standard (DES) algorithm.

Referring to claims 6, 24, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as 3DES (Figures 5 & 8), which meets the limitation of one of a plurality of cryptographic algorithms comprises the Triple-DES algorithm.

Referring to claims 7, 20, 25, Kessler does not specify that the co-processor utilizes the x86 instruction set. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14).

Referring to claims 8, 9, Kessler discloses that each execution unit includes a register file block that includes that data to be operated on by the corresponding cryptographic algorithm (Figure 8 & Co. 9, lines 18-40), which meets the limitation of said single, atomic cryptographic instruction implicitly references a plurality of registers within said microprocessor, a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said encryption operation is to be accomplished. Kessler does not specify that the co-processor utilizes the x86 instruction set. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14).

Referring to claim 10, Kessler discloses that each execution unit includes a register file block that includes that data to be operated on by the corresponding cryptographic algorithm (Figure 8 & Co. 9, lines 18-40), which meets the limitation of a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said encryption operation upon a plurality of input text blocks.

Referring to claim 11, Kessler discloses that each execution unit includes a register file block that includes that data to be operated on by the corresponding cryptographic algorithm

(Figure 8 & Co. 9, lines 18-40), which meets the limitation of a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

Referring to claim 12, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4 (Figures 5 & 8), which meets the limitation of a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said encryption operation.

Referring to claim 13, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as RC4 (Figures 5 & 8), which meets the limitation of a fifth register, wherein contents of said fifth register comprises a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector comprising an initialization vector or initialization vector equivalent for use in accomplishing said encryption operation.

Referring to claim 14, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4 (Figures 5 & 8), which meets the limitation of a sixth register, wherein contents of said sixth register comprises a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said encryption operation because Applicant's specification essentially states that the control word identifies the algorithm (Page 38, paragraph 55).

Referring to claim 15, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as 3DES, DES (Figures 5 & 8), which meets the limitation of a cryptographic unit executes a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptographic unit.

Referring to claim 16, Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8 & Col. 4, lines 12-13), which meets the limitation of a cryptographic unit configured to execute a decryption operation responsive to receipt of a single, atomic cryptographic instruction that prescribes said decryption operation wherein said single, atomic cryptographic instruction is one of the instructions in an application program that are fetched from memory by fetch logic in said microprocessor. The execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of an algorithm field, configured to prescribed one of a plurality of cryptographic algorithms to be employed when executing said decryption operation. Using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9, lines 28-43), which meets the limitation of algorithm logic, operatively coupled to said cryptography unit, configured to direct said microprocessor to perform said decryption operation according to said one of the plurality of cryptographic algorithms. Kessler does not specify that the co-processor executes that program

that includes the cryptographic operations. Colavin discloses a host and co-processor configuration wherein the co-processor executes the actual application program (Abstract & [0018]), which meets the limitation of wherein said microprocessor executes said application program to obtain expected results. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor of Kessler to execute the actual application program as described by Colavin in order to efficiently execute programs with high instruction level parallelism as taught by Colavin ([0002]). Kessler does not specify that the co-processor utilizes the x86 instruction set. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14). Applicant's specification shows that integer instructions are inherent to the x86 instruction set (Page 27). Therefore, when implementing the x86 instruction set in the co-processor of Kessler, as previously described, the execution units would effectively operate as a "integer unit" as claimed.

Referring to claim 17, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as AES (Figures 5 & 8), which meets the limitation of one of a plurality of cryptographic algorithms comprises the Advanced Encryption Standard (AES) algorithm.

Referring to claim 18, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as DES (Figures 5 & 8), which meets the limitation of one of a

plurality of cryptographic algorithms comprises the Digital Encryption Standard (DES) algorithm.

Referring to claim 19, Kessler discloses that the operation blocks correspond to cryptographic algorithms such as 3DES (Figures 5 & 8), which meets the limitation of one of a plurality of cryptographic algorithms comprises the Triple-DES algorithm.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/

Primary Examiner, Art Unit 2432